(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－175224
（P2002－175224A）
(43)公開日　平成14年６月21日(2002.6.21)

(51)Int.Cl.⁷	識別記号	FI	テーマコード(参考)
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ　５Ｂ０８９
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　12/46	Ｅ　５Ｋ０３０
12/66		12/66	Ｂ　５Ｋ０３３

審査請求　有　　請求項の数７　ＯＬ　（全　６　頁）

(21)出願番号　特願2000－371240(P2000－371240)

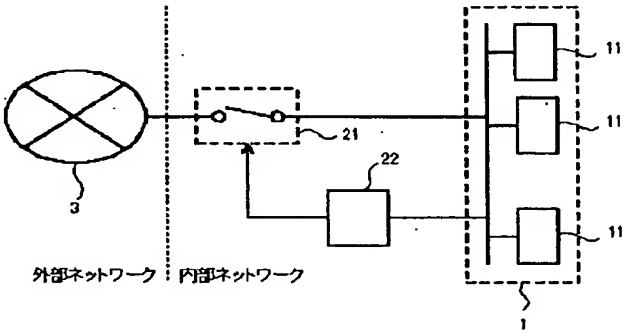
(22)出願日　平成12年12月６日(2000.12.6)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　白川　洋一
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100095407
弁理士　木村　満

Ｆターム(参考)　5B089 GA31 HA06 KA17 KB13 KC52
KC54 KG10
5K030 GA15 HA08 HC01 HC14 HD03
HD06 KA13 LB03 LC16 LD20
5K033 AA08 BA17 CB03 CB08 DA01
DA06 DB03 DB18 DB20 EA07

(54)【発明の名称】　ネットワーク接続システム、及び装置

(57)【要約】
【課題】　内部ネットワークに接続された計算機に対して、外部ネットワークからの不正なアクセスを防ぐと共に、内部ネットワーク内でのデータのやりとりを効率的に行う。
【解決手段】　狭い意味での内部ネットワークとしてのＬＡＮ１と、外部ネットワークとしてのＷＡＮ３との間に、回線スイッチ部２１が設けられている。回線スイッチ部２１は、制御部２２の制御によって接続状態と切断状態とが切り替えられ、切断状態となると、ＷＡＮ３からＬＡＮ１内の計算機１１へのアクセスが不可能となる。回線スイッチ部２１が切断状態となった場合においても、ＬＡＮ１内の各計算機１１同士は、接続状態にあり、自由にデータのやりとりを行うことができる。



【特許請求の範囲】
【請求項１】複数の計算機を有する内部ネットワークと、該内部ネットワークを外部ネットワークに接続するためのネットワーク接続装置を備えるネットワーク接続システムであって、
前記ネットワーク接続装置は、
一端が前記内部ネットワークに、他端が前記外部ネットワークに接続され、前記内部ネットワークと前記外部ネットワークとを実質的な接続状態と実質的な切断状態とのいずれかに切り替えるスイッチ手段と、
所定の条件が成立することによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替える制御手段とを備えることを特徴とするネットワーク接続システム。
【請求項２】前記内部ネットワークと前記外部ネットワークとの間に、前記外部ネットワークから前記内部ネットワークへのアクセスをチェックし、該アクセスが不正アクセスである場合に内部ネットワークへのアクセスを制限するファイアウォールをさらに備えることを特徴とする請求項１に記載のネットワーク接続システム。
【請求項３】前記内部ネットワークと前記外部ネットワークとは、前記外部ネットワークから前記内部ネットワークへの不正アクセスがあった場合にアラームを発生するアラーム発生手段を含むファイアウォールを介して接続されており、
前記ネットワーク接続装置は、前記ファイアウォール内の機能として実現されており、
前記制御手段は、前記アラーム発生手段がアラームを発生した場合に、前記スイッチ手段を実質的な切断状態とすることを特徴とする請求項１に記載のネットワーク接続システム。
【請求項４】複数の計算機を有する内部ネットワークを、外部ネットワークに接続するためのネットワーク接続装置であって、
一端が前記内部ネットワークに、他端が前記外部ネットワークに接続され、前記内部ネットワークと前記外部ネットワークとを実質的な接続状態と実質的な切断状態とのいずれかに切り替えるスイッチ手段と、
所定の条件が成立することによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替える制御手段とを備えることを特徴とするネットワーク接続装置。
【請求項５】前記スイッチ手段及び前記制御手段は、それぞれ前記外部ネットワークから前記内部ネットワークへの不正アクセスがあった場合にアラームを発生するアラーム発生手段を含むファイアウォールの機能として実現されており、
前記制御手段は、前記アラーム発生手段がアラームを発生した場合に、前記スイッチ手段を実質的な切断状態とすることを特徴とする請求項４に記載のネットワーク接続装置。
【請求項６】前記制御手段は、前記内部ネットワークにおける所定の事象の発生を監視し、該所定の事象の発生によって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替えることを特徴とする請求項４または５に記載のネットワーク接続装置。
【請求項７】前記制御手段は、計時手段によって計時された時間が所定の時間となることによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替えることを特徴とする請求項４乃至６のいずれか１項に記載のネットワーク接続装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＬＡＮ（Local Area Network）などの内部ネットワークと、ＷＡＮ（Wide Area Network）などの外部ネットワークとを接続するネットワーク接続システム及び装置に関する。
【０００２】
【従来の技術】近年、多くの計算機が何らかの形でネットワーク接続されて使用されるようになってきているが、各計算機への不正アクセスを如何にして防ぐかが大きな課題となっている。特にＬＡＮなどの内部ネットワークと、インターネットを始めとするＷＡＮなどの外部ネットワークとが接続されているネットワークシステムでは、一般に、内部ネットワークと外部ネットワークとの間にファイアウォールを設け、ファイアウォールによる認証やフィルタリングによって、各計算機が外部ネットワークから不正にアクセスされるのを防いでいる。
【０００３】ところが、ファイアウォールを介したネットワーク接続システムでも、内部ネットワークに接続された各計算機は、基本的には外部ネットワークとも常時接続されていることとなる。このため、外部ネットワークからの不正アクセスを完全に遮断するのは不可能であった。そこで、各計算機において外部からの不正アクセスを防止するための技術として、特開２０００－１０８８７号公報においてセキュリティスイッチ付きネットワークインタフェースモジュールが提案されている。
【０００４】図４は、特開２０００－１０８８７号公報に記載のセキュリティスイッチ付きネットワークインタフェースモジュールを示すブロック図である。図示するように、ネットワークインタフェースモジュール１０１は、計算機１０５に１対１で対応して設けられるものであり、ネットワークインタフェース１０２と、セキュリティスイッチ１０４を含む電源インタフェース１０３とから構成されている。
【０００５】ネットワークインタフェースモジュール１０１の電力は、計算機１０５内の電源１０７から供給されている。ＣＰＵ１０６が電源１０７からの電力の供給を停止すると、セキュリティスイッチ１０４がオフし、ネットワークインタフェース１０２が動作不能となる。

これにより、外側のネットワークから計算機１０５にアクセスすることが不可能になり、計算機１０５への不正アクセスを防ぐことができるようになっている。

【０００６】

【発明が解決しようとする課題】しかしながら、特開２０００－１０８８.7号公報に記載の技術では、ネットワークインタフェースモジュール１０１をそれぞれの計算機１０５に対応して設けなければならない。ところが、内部ネットワークと、外部ネットワークとが接続されたシステムでは、内部ネットワークからの計算機１０５への不正アクセスはあまり考えられない。このようなほとんど考えられないような不正アクセスに対して、計算機１０５の各々に冗長構成をするというのは、スペース及びコストの面から無駄である。

【０００７】また、内部ネットワークと、さらに外部ネットワークに接続された計算機にあっては、通常、内部ネットワーク内でのデータのやりとりは頻繁に行われるが、これに対して外部ネットワークとのデータのやりとりは圧倒的に少ない。このため、特開２０００－１０８７号公報のように計算機１０５の各々に対してネットワークインタフェースモジュール１０１を設け、計算機１０５の各々がアクセス拒否できるようにすると、内部ネットワーク内のみでのデータのやりとりに支障が生じてしまう可能性がある。

【０００８】本発明は、内部ネットワークに接続された計算機に対して、外部ネットワークからの不正なアクセスを防ぐと共に、内部ネットワーク内でのデータのやりとりを効率的に行い得るネットワークアクセスシステム等を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するため、本発明の第１の観点にかかるネットワーク接続システムは、複数の計算機を有する内部ネットワークと、該内部ネットワークを外部ネットワークに接続するためのネットワーク接続装置を備えるネットワーク接続システムであって、前記ネットワーク接続装置は、一端が前記内部ネットワークに、他端が前記外部ネットワークに接続され、前記内部ネットワークと前記外部ネットワークとを実質的な接続状態と実質的な切断状態とのいずれかに切り替えるスイッチ手段と、所定の条件が成立することによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替える制御手段とを備えることを特徴とする。

【００１０】上記のネットワーク接続システムでは、制御手段がスイッチ手段を実質的な切断状態とすることによって、外部ネットワークから内部ネットワークへのアクセスが不能となる。これにより、外部ネットワークから内部ネットワークへの不正アクセスを遮断することが可能となる。ここで、スイッチ手段が実質的な切断状態となっている場合でも、内部ネットワーク内の計算機同士は、互いに接続状態を保ったままであり、内部ネットワーク内でのデータのやりとりに支障が生じることはない。

【００１１】上記ネットワーク接続システムは、前記内部ネットワークと前記外部ネットワークとの間に、前記外部ネットワークから前記内部ネットワークへのアクセスをチェックし、該アクセスが不正アクセスである場合に内部ネットワークへのアクセスを制限するファイアウォールをさらに備えるものとすることができる。

【００１２】上記ネットワーク接続システムにおいて、前記内部ネットワークと前記外部ネットワークとは、前記外部ネットワークから前記内部ネットワークへの不正アクセスがあった場合にアラームを発生するアラーム発生手段を含むファイアウォールを介して接続されたものであってもよい。この場合において、前記ネットワーク接続装置は、前記ファイアウォール内の機能として実現されたものとすることができ、前記制御手段は、前記アラーム発生手段がアラームを発生した場合に、前記スイッチ手段を実質的な切断状態とすることができる。

【００１３】これら示したように、スイッチ手段に加えてファイアウォールを併用することによって、外部ネットワークから内部ネットワークへの不正アクセスをより強固に防止することができ、さらにセキュリティの高いシステムを構築することが可能となる。

【００１４】上記目的を達成するため、本発明の第２の観点にかかるネットワーク接続装置は、複数の計算機を有する内部ネットワークを、外部ネットワークに接続するためのネットワーク接続装置であって、一端が前記内部ネットワークに、他端が前記外部ネットワークに接続され、前記内部ネットワークと前記外部ネットワークとを実質的な接続状態と実質的な切断状態とのいずれかに切り替えるスイッチ手段と、所定の条件が成立することによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替える制御手段とを備えることを特徴とする。

【００１５】上記ネットワーク接続装置において、前記スイッチ手段及び前記制御手段は、それぞれ前記外部ネットワークから前記内部ネットワークへの不正アクセスがあった場合にアラームを発生するアラーム発生手段を含むファイアウォールの機能として実現されたものであってもよい。この場合において、前記制御手段は、前記アラーム発生手段がアラームを発生した場合に、前記スイッチ手段を実質的な切断状態とすることができる。

【００１６】上記ネットワーク接続装置において、前記制御手段は、また、前記内部ネットワークにおける所定の事象の発生を監視し、該所定の事象の発生によって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替えるものとすることもできる。

【００１７】上記ネットワーク接続装置において、前記

制御手段は、さらに、計時手段によって計時された時間が所定の時間となることによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替えるものとすることもできる。

【００１８】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態について説明する。

【００１９】図１は、この実施の形態にかかるネットワーク接続システムの構成を示すブロック図である。図示するように、このネットワーク接続システムでは、内部ネットワークとしてのＬＡＮ１に、複数の計算機１１が接続されている。ＬＡＮ１は、回線スイッチ部２１と、制御部２２とに接続されている。回線スイッチ部２１及び制御部２２は、広い意味での内部ネットワークに含まれる。回線スイッチ部２１の他端は、外部ネットワークとしてのＷＡＮ３に接続されている。なお、具体的に述べると、ＬＡＮ１はイントラネット、ＷＡＮ３はインターネットとすることができる。

【００２０】回線スイッチ部２１は、制御部２２から送られた制御信号に基づいて、ＬＡＮ１とＷＡＮ３との間を接続状態とするか、切断状態とするかを切り替える。制御部２２は、ＬＡＮ１から得られる制御信号に基づいて、回線スイッチ部２１の状態を切り替える制御信号を生成し、出力する。

【００２１】制御部２２は、例えば、ＬＡＮ１に接続する回線ボードと、回線スイッチ部２１を制御するパーソナルコンピュータ等で実現することができる。この場合、回線スイッチ部２１は、シリアル信号によってＬＡＮ１とＷＡＮ３とを物理的にＯＮ／ＯＦＦするケーブルスイッチであってもよい。また、回線スイッチ部２１と制御部２２は、専用のハードウェア装置で実現してもよい。この場合、ＬＡＮ１に接続するインタフェースとＷＡＮ３に接続されるインタフェースとが提供されていればよいこととなる。

【００２２】以下、このネットワーク接続システムにおける動作について説明する。ここで、通常の状態では、回線スイッチ部２１は切断状態になっているものとする。

【００２３】ＬＡＮ１をＷＡＮ３と接続すべき事象、例えば、計算機１１のいずれかがＷＡＮ３上のコンピュータ装置にアクセスし、データを取得しようとする事象が発生したときに、当該計算機１１は、制御部２２にＷＡＮ３にアクセスしようとする旨を通知する。この通知に基づいて、制御部２２は、回線スイッチ部２１に制御信号を送り、回線スイッチ部２１を接続状態に切り替えさせる。

【００２４】回線スイッチ部２１が接続状態となった後、当該計算機１１は、ＷＡＮ３上のコンピュータ装置にアクセスし、そこからデータを取得する。データの取得が終了すると、当該計算機１１は、制御部２２にＷＡＮ３へのアクセスを終了した旨を通知する。この通知に基づいて、制御部２２は、回線スイッチ部２１に制御信号を送り、回線スイッチ部２１を切断状態に切り替えさせる。

【００２５】一方、ＷＡＮ３上のコンピュータ装置がＬＡＮ１内の計算機１１のいずれかにアクセスしようとしたとき、通常、回線スイッチ部２１は切断状態となっているので、実際には計算機１１にアクセスすることができない。この状態においても、ＬＡＮ１内の計算機１１同士は接続状態となっているため、互いに自由にデータをやりとりすることができる。

【００２６】以上説明したように、この実施の形態にかかるネットワーク接続システムでは、制御部２２が回線スイッチ部２１を切断状態としていれば、ＷＡＮ３からＬＡＮ１内の計算機１１にアクセスすることができない。このため、ＬＡＮ１内の計算機１１が外部ネットワークとしてのＷＡＮ３とデータをやりとりする必要がない場合は、回線スイッチ部２１を全て切断状態としておけばよいので、ＷＡＮ３からＬＡＮ１内の計算機１１に不正にアクセスされるのを防ぐことができる。

【００２７】また、回線スイッチ部２１が切断状態にある場合でも、ＬＡＮ１内の計算機１１同士は、常に接続状態を保つことができている。このため、ＬＡＮ１内における計算機１１同士のデータのやりとりに支障が生じることはなく、ＬＡＮ１内における処理を効率的に行うことができる。

【００２８】本発明は、上記の実施の形態に限られず、種々の変形、応用が可能である。以下、本発明に適用可能な上記の実施の形態の変形態様について説明する。

【００２９】上記の実施の形態では、制御部２２は、内部ネットワークであるＬＡＮ１内において発生した事象に基づいて、回線スイッチ部２１を接続状態と切断状態のいずれかに切り替えていた。これに対して、外部ネットワークであるＷＡＮ３において発生した事象によっても、回線スイッチ部２１を切り替えることは可能である。もっとも、ＷＡＮ３において発生した事象は、回線スイッチ部２１が接続状態にある場合しか制御部２２に伝えられないが、制御部２２は、ＷＡＮ３において発生した事象に基づいて回線スイッチ部２１を適切なタイミングで接続状態から切断状態に切り替えることができる。

【００３０】また、制御部２２による回線スイッチ部２１の接続状態と切断状態との切り替えは、タイマが計時する時間によって行うことも可能である。例えば、同期的なアプリケーションや、メールやニュースの配送、ファイルの転送やバックアップ等は、必ずしも常時接続しなければ行い得ないものではない。そこで、タイマが計時する時間に従って、予め定められた時間帯で回線スイッチ部２１を接続状態とし、このようなデータの授受を行うものとすればよい。なお、タイマは、制御部２２自

体が備えるものとしても、制御部２２の外側にあり、時間情報を制御部２２に入力可能にしたもののいずれであってもよい。

【００３１】上記の実施の形態では、ＬＡＮ１とＷＡＮ３とは、回線スイッチ部２１を介してのみ接続されるものとしていた。これに対して、ＬＡＮ１とＷＡＮ３との接続に、ファイアウォールを併用した構成のネットワーク接続システムも構成することが可能である。

【００３２】図２は、ファイアウォールを併用した、他の構成のネットワーク接続システムの構成を示すブロック図である。このネットワーク接続システムでは、回線スイッチ部２１とＬＡＮ１との間に、さらにファイアウォール２３が設けられている。もっとも、ファイアウォール２３の位置は、回線スイッチ部２１とＷＡＮ３との間であってもよい。

【００３３】図２のネットワークシステムにおいて、ＷＡＮ３からＬＡＮ１内の計算機１１に不正アクセスがあったとする。ここで、回線スイッチ部２１が接続状態となっていると、その不正アクセスは、ファイアウォール２３にまで達する。次に、ファイアウォール２３は、ＷＡＮ３からのアクセスをフィルタにかけるが、不正アクセスであるために、ＬＡＮ１内の計算機１１に伝えない。このような構成により、ＷＡＮ３からＬＡＮ１内の計算機１１への不正アクセスの防止が強化され、上記の実施の形態で示したシステムよりも、一層セキュリティの高いシステムを構築することができる。

【００３４】図３は、ファイアウォールを併用した、さらに他の構成のネットワーク接続システムの構成を示すブロック図である。このネットワーク接続システムでは、ＬＡＮ１とＷＡＮ３とはファイアウォール２を介して接続されており、回線スイッチ部２１及び制御部２２は、ファイアウォール２の機能として実現されている。ファイアウォール２は、ＷＡＮ３からＬＡＮ１内の計算機１１に不正アクセスがあった場合に、アラームを発するアラーム発生部２４を含んでいる。

【００３５】ここで、制御部２２は、アラーム発生部２４がアラームを発生したとき、ＬＡＮ１とＷＡＮ３とが切断状態となるように、回線スイッチ部２１に制御信号を送る。回線スイッチ部２１が切断状態に切り替えられた後、例えば、ＬＡＮ１内の計算機１１からＷＡＮ３へのアクセスがあった場合に、制御部２２は、再び接続状態となるよう回線スイッチ部２１に制御信号を送ることができる。なお、制御部２２は、アラーム発生部２４がアラームを発生した場合の他に、上記したような種々の事象が発生したときにも、回線スイッチ部２１を切断状態に切り替えるように制御することができる。

【００３６】このような構成としたことで、ＷＡＮ３からＬＡＮ１内の計算機１１へ不正なアクセスがあった場合には、ファイアウォール２としてその不正アクセスを伝えないだけでなく、回線スイッチ部２１も切断状態とされるので、不正アクセスの防止をより強化することができる。これにより、上記の実施の形態で示したシステムよりも、一層セキュリティの高いシステムを構築することができる。

【００３７】上記の実施の形態では、ＬＡＮ１を内部ネットワークとし、これに外部ネットワークとしてのＷＡＮ３が接続されたネットワーク接続システムを例として説明した。しかしながら、例えば、ＬＡＮとＬＡＮとをルータなどにより接続したネットワークシステムにおいてでも、そのうちのいずれか１以上のＬＡＮにおいて、上記した回線スイッチ部２１と制御部２２とを設けることができる。

【００３８】

【発明の効果】以上説明したように、本発明によれば、内部ネットワークに接続された各計算機に対して、外部ネットワークからの不正なアクセスを防止できると共に、内部ネットワーク内でのデータのやりとりを支障なく行うことができる。

【図面の簡単な説明】

【図１】本発明の実施の形態にかかるネットワーク接続システムの構成を示すブロック図である。

【図２】本発明の他の実施の形態にかかるネットワーク接続システムの構成を示すブロック図である。

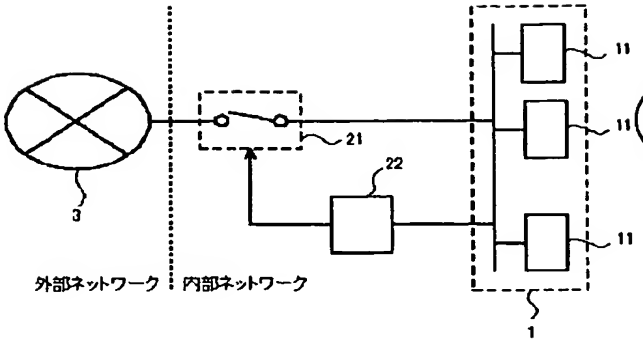
【図３】本発明の他の実施の形態にかかるネットワーク接続システムの構成を示すブロック図である。

【図４】従来例にかかるセキュリティスイッチ付きネットワークインタフェースモジュールを示すブロック図である。

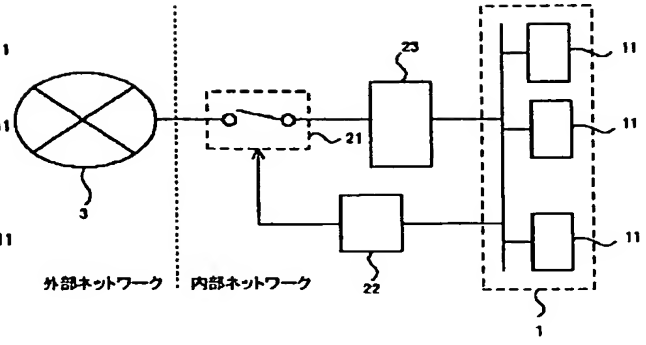
【符号の説明】

１　ＬＡＮ
２　ファイアウォール
３　ＷＡＮ
１１　計算機
２１　回線スイッチ部
２２　制御部
２３　ファイアウォール
２４　アラーム発生部

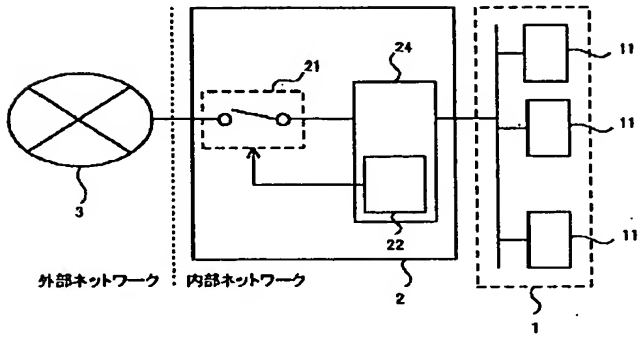
【図１】


11
11
11
21
22
3
外部ネットワーク
内部ネットワーク
1

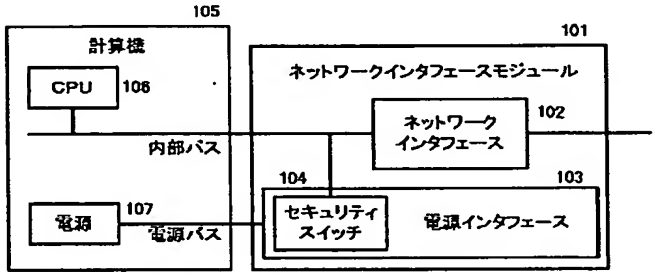
【図２】


23
11
11
11
21
3
外部ネットワーク
内部ネットワーク
22
1

【図３】


21
24
11
11
11
3
22
外部ネットワーク
内部ネットワーク
2
1

【図４】


105
計算機
CPU
106
内部バス
電源
107
電源バス
101
ネットワークインタフェースモジュール
ネットワーク
インタフェース
102
104
103
セキュリティ
スイッチ
電源インタフェース